Analysis of Duo Mobile Application on Enhancing User Authentication in Cloud Computing

Nor Fazalina Binti Azman

Faculty of Electrical Engineering
University of Technology MARA
Shah Alam, Malaysia
azza_keai@yahoo.com

Abstract— **Cloud computing is an IT service that can access remotely at any time and from anywhere through the internet. In order to secure data stored in the cloud, an efficient authentication method must be considered to overcome the security concerns. This project proposed the used of duo mobile application software as a second layer of authentication and the application is installed in the mobile device prior to login to the web page. The proposed technique is proven to mitigate few types of attacks such as Man-in-the-Middle (MITM) and session cookies stolen.**

Keywords— **Cloud Computing; User Authentication; Second Layer of Authentication; Duo Mobile Application; Mobile Devices.**

I. INTRODUCTION

Cloud computing is one of the new IT services that has moved rapidly during recent years. It means 'internet computing' that users can access and store data from anywhere and anytime in the open internet. There are many advantages of this technology, however it also has some weaknesses especially in the area of security and privacy. Authentication is the first step towards secure environment in cloud computing.

Authentication is a process to verify the identity users. When the users decided to use cloud services, they will have to store a password in multiple cloud, so that the mere copy of the user's information will be in the database and also the user needs to exchange the authentication information. This redundant action may lead to an exploitation of authentication mechanism. Therefore, the main security issue in cloud computing is a user authentication [1].

In this paper, one method is proposed and implemented to authenticate cloud computing using duo layer authentication as a solution of security issue. This approach verifies user authenticity using mobile phone followed by entering the username and password as usual. It gives more security through a double authentication process which is a second layer security. This will give extra hardness to the attackers to steal the data and to protect the network resources. Following section discuss the implementation followed by analysis and conclusion.

II. PROBLEM STATEMENT

The benefit that could services offer is undeniable. However, they are always second thought when the users want to use the cloud services. The main reasons in the security issue in order to protect the data, users usually used username and password. However, this information in accessible or available to the cloud service provider. This has reduce public's user interest in using cloud services. Apart from that, usually the login to the cloud services uses similar login and password as email services. This has further expose the cloud services to data breach problems.

III. RELATED WORKS

Cloud computing is a new change in IT industry and academic research. It offers a set of resources and services over the internet and also involves virtualization. It is a hot topic to be discussed the technology and strategy, including risk assessment, compliance and audit [2]. However, in the development of the cloud computing, it faced security issues with the growing popularity of cloud computing. In 2009, Gartner survey showed that more than 70 percent of users do not intend to use cloud computing because of the data security and privacy. Hence, it must be handled with variables of measures and methods to solve these problems.

Since the development of cloud computing moves rapidly, there are many benefits and advantages can be listed. For example, it is effortless setup, low cost, scalable, reliable and widely accessible. However, many problems also move simultaneously with that caused by weak authentication process and confidential techniques in protecting users' sensitive information in the very open internet [3].

Z. Javaid suggests methods and techniques to overcome the risks, especially hiding credential authentication travels around the world [4]. Thus, many techniques can be used to strengthen the authentication process such as prevent the data from being stolen and exposed to non-legitimate users, but still having the complexity to overcome. So that, the combination between the Kerberos server and VPN supported firewall can be implemented which is the first level of authentication were taken over by VPN and the second level

authentication can be done using Kerberos server. They proposed another technique called by RADIUS integration to measure the performance analysis of suggested model against the conventional model using multiple parameters.

One of the security tools in cloud computing is a user authentication scheme which involves 3 items which are authentication, authorization and accounting. However, most of this scheme has some security issues and hardly implemented. Therefore, J. Yanget proposed an ID-based user authentication scheme for cloud. The scheme offers few advantages such as low computation cost, effortless implementation, low storage space and reduce the verification time [5]. In other words, this scheme is more practical and very efficient rather than Wang et al.'s scheme and Lee et al.'s scheme which is it cannot prevent the impersonation message attack and alteration attack.

Proofing the identities using authentication process is a key technology for security. Today, traditional password authentication is still relevant to use. However, with the advance in hackers' technology and huge demand for cloud services, extra effort needs to be put into ensuring a stronger authentication level. In his paper proposed a multi-factor authentication framework for cloud [6]. This framework introduces Cloud Access Management (CAM) system that combines arithmetic captcha encryption process and secret splitting. Process arithmetic captcha involves two operands and one operator that the server will be generates randomly and display to the user as a normal captcha.

Security, sharing, authenticity and integrity are a must in cloud computing. The security demands differ for the public and private cloud. Public cloud offers data to unlimited internet users while private cloud limits access to online data to specific users only. Authentication, another work by K. Chachapara proposed the used of cryptography algorithms such as AES and RSA in the authentication algorithm [7]. The author also implements different key for different users and decided by the user. They also concerned about how to mitigate security issues such as authentication, data protection and transmit process of secured data. The encryption process can solve the issue either in authentication problems or data protection problems.

This presents encrypt and exchange key by using the Diffie-Helmen and RSA small-e which is evaluated and examine based on four parameters like time, key size, correctness and security. As a result, the objectives have been achieved to increase data protection and to decrease security risks at the same time [8].

A. Dubey proposed two-way communications which involved client and cloud environment admin [9]. RSA and MD5 algorithms have been applied to protect the data from the admin and hide the data of users. For example, if a user uploads the data, it automatically encrypts using RSA algorithm and then in the admin side, it supposedly decrypts the uploaded data using their own private key. It is believed that encryption, decryption and message digest can fulfill the needs for security and also effective in today's era of globalisation.

C. Xue-Zhou in this paper tried to specify and optimise encryption process of users for sensitive data [10]. It proposed two technologies which are double encryption and check of the message. Furthermore, it can overcome the problem issues and ensure the integrity, safety and effectiveness of data. Then, encryption symmetric key is a process of double encryption technology. Firstly, the client must generate a symmetric key and digest the message and the last process is adding in the behind messages encrypted transmission together.

All this problem can come up with a solution to get effective cloud computing and data encryption is the most effective method to use. Finally, a lot of researchers having a lot of methods and techniques can be used in nowadays. Therefore, both sides between users and service provider are very important acts together in handling on security issues and data protection in cloud computing [11].

N. Yildirim proposed method using Samsung Galaxy S5 fingerprint recognition feature and International Equipment Identity (IMEI) number to generate single time password [12]. This feature develops a web login authentication mobile application via their software development kits (SDKs). The main purpose is to give more secure and practical solution for identification on mobile devices. In addition, now days, mobile devices have become an important part and one of the popular gadget of human life. For example, the users in the world must accesss their email, social networks, banking process and others via mobile devices only. This method can be used to previous activities that we discuss before this which are used to sign in or log in to many online accounts.

Biometrics recognition systems can be listed as iris, face, retina, fingerprint, voice, signature, keystroke and others. In this study, they use the fingerprint features because of high in terms of ensuring the security of application. And then, this method cannot be shared with others and get distinguish between others by the unique of those ridges. Although, this method have some weakness because they just implement that in the Samsung devices and android software. This question is how people that using Apple or other software. This paper decided that secure access to medical records is the main challenge. Users will be remote health framework to monitor their patients. There is a growing demand to store data in the cloud with an increase in the amount of digital content. T. Bhattasali proposed two factor authentication mechanism to ensure high accuracy level [13]. We know that biometrics authentication is more reliable than traditional method because of its uniqueness and low intrusiveness. This method divided into two factors which are first factor and second factor. The first authentication is use biometrics keystroke analysis model and the second factor is using secret PIN mechanism. It is different with our proposed on both factors.

Suggests two factor authentication using camera features to secure and strong their access applied to web authentication. Camera authentication (CamAuth) is a method

that used for this project [14]. In CamAuth, a mobile device is used as the second authentication factor to verify identity who is login a web from a PC. Then, it can communicate directly with the PC through the secure visible light communication channels, which incurs no cellular cost and is immune to radio frequency attacks. The purpose is to ensure the security of web authentication strongly and securely also counter various password attacks especially MITM and phishing attacks.

Z. Abduljabbar proposed that robust scheme to protect authentication to protect authentication in cloud computing. It is to ensure message/image document integrity for each user's login by providing one-time biometric message/image authentication code called MACLESS. In addition, this study is to prevent common forms of attack such as forgery, stolen verifier, brute force, replay, insider attacks and others. MACLESS is a summation of combining the key-based hash function. At the end of this experiment, it will prove that the invulnerability and efficiency of the proposed scheme [15].

This paper was proposed the cloud storage identity design based on fingerprint identification because of username and password usually people easy to remember and easy to crack by attacker [16]. Other than that, the impact of this method is given to enhancing the reliability, safety and it get prevent illegal accessing from anonymous. It involved storage devices as the core through applying software accessing provides data storage and business services.

For this project, the hybrid model with combination of auto complete function of the browser was proposed [17]. The fingerprint inbuilt in certain mobile devices like Samsung Galaxy which is triggered automatically the fingerprint recognition module when the user visits certain websites which is offer login options and not others. The result is on a browser enabled by the system to study average response times, accuracy and effect on browser performance.

This study proposes two-factor authentication (2FA) access control system fir web-based cloud computing services [18]. It can enhance the security of the system, especially in those cases where many users share the same machine. It also gives restricted access function for privacy purpose. Simulate the prototype of the protocol practicability also showing in this project.

'Cloud of Things' arises some challenges in terms of user access control and outsourced data integrity and privacy protection as the data owner has no more the physical control of his data. In this paper, 'sensor cloud' designs with a new security architecture to securely store and process sensed data [19]. Other than that, it proposes attribute-based encryption (ABE) paring with cryptosystem (PBC) and lightweight token based authentication algorithm (ECDSA) to secure and efficient data owner access-controlled purpose. Other than that, if gives the effectiveness of solution in terms of computation and storage cost.

TPA is leased by the provider and after a time cloud service provider may contract with the TPA to conceal the loss of data from the user to prevent the defamation. This paper presents a novel secure cloud storage system to ensure the protection of organizations' data from both the cloud provider and the third party auditor and from some users who take advantage of the old accounts to access the data stored on the cloud. The proposed system enhances the authentication level of security by using two authentication techniques; Time-based One Time Password (TOTP) for cloud users verification and Automatic Blocker Protocol (ABP) to fully protect the system from unauthorized third party auditor [20]. The experimental results demonstrate the effectiveness and efficiency of the proposed system when auditing shared data integrity.

As a conclusion, the growing demand in cloud computing has increase the security concerns. From all related works, it can be concluded that duo mobile application software is still not been highlighted as a security method either in the first or second layer for user authentication in cloud computing.

IV. METHODOLOGY : DUO MOBILE APPLICATION SOFTWARE

The tool to fulfill this project is applied by using duo mobile application software as a second level of security as shown in Figure 1. This application is installed in the mobile device prior to login to the webpage.

Fig. 1. Duo mobile Application software

Duo security is a two-step verification that provides additional security to pairing with the username and password for allowing access. Figure 2 briefly depicts the basic of two step user verification. The user's enter the username and password as normally (first layer of security). And then, for the second layer of security, the identity of the user is verified using mobile devices. Upon successful, the user will login securely.

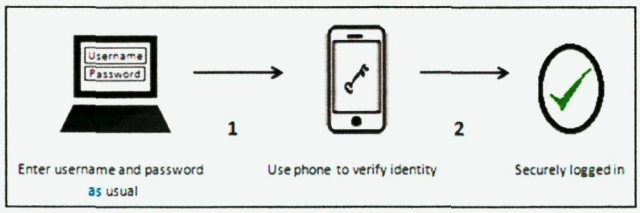

Fig. 2. Two step user verification

The flowchart and pseudocode of duo security are discussed.

A. *Flowchart of User Verification Process*

This section briefly explain the operation of the duo mobile application. The flowchart of the user verification process can be seen on Figure 3. The processes include registration to login as a new user or first time login process and also is login as an existing user.

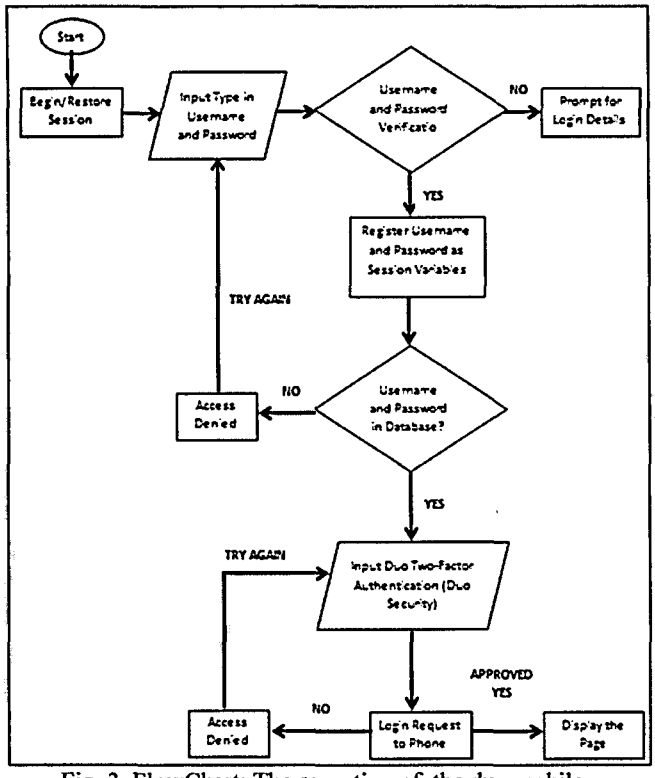

Fig. 3. FlowChart: The operation of the duo mobile application

The operation of the duo mobile application as follows:

1) Part I : Login in the first layer of security - User needs to register if there is no record in the database. Registration of the user's mobile phone number is required as their mobile phone number.The user enters the username and password as normally.

2) Part II : Verification in the second layer of security – The identity of the user is verified to login more securely. There are three options for authenticating users such as duo push-notification, phone callback or SMS passcode generated on a mobile phone. The web application will receive an authentication response. At the end of process, the web application is protected and securely log in by combining of two layers of security.

B. *Pseudocode of Duo Security*

Pseudocode of duo security has been configured and added to the web application's programming as shown in Figure 4.

```
if (isset ($_POST['sig_response']))
{
$resp = Duo\Web::verifyResponse(IKEY, SKEY, AKEY, $_POST['sig_response']);
        if ($resp === $_SESSION ['user'])
        {
        $_SESSION ['login'] = "Y";
        header ('Location: welcome.php');
        }
}
```

Fig. 4: Pseudocode for duo mobile application software

IKEY, SKEY and HOST are best stored outside of the webroot in a production implementation. This is the coding to verify sig response and log in user. Then, ensure that VerifyResponse returns the username user logged in with instead of complete the login process.

V. RESULT AND ANALYSIS

This section discusses the data analysis that are divided into two parts which are the operation of the application and the authentication method.

A. *Operation of Application*

The operation of the duo mobile application as follows:

1) Registration – User needs to register if there is no record in the database. Registration of the user's mobile phone number is required as their mobile phone number shown in Figure 5.

2) Login in the first layer of security - The user enters the username and password as normally as shown in Figure 6.

3) Verification in the second layer of security – The identity of the user is verified to login more securely. There are three options for authenticating users such as duo push-notification, phone call or a one time passcode generated on a mobile phone shown in Figure 7.

4) Login successful - The web application will receive an authentication response. At the end of process, the web application is protected and securely log in by combining of two layers of security shown in Figure 8.

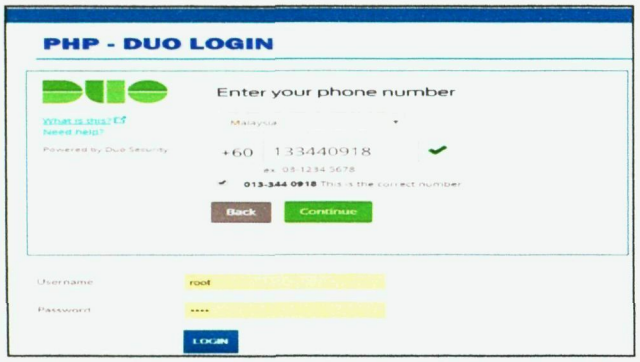

Fig. 5. Registration of duo mobile application for new user

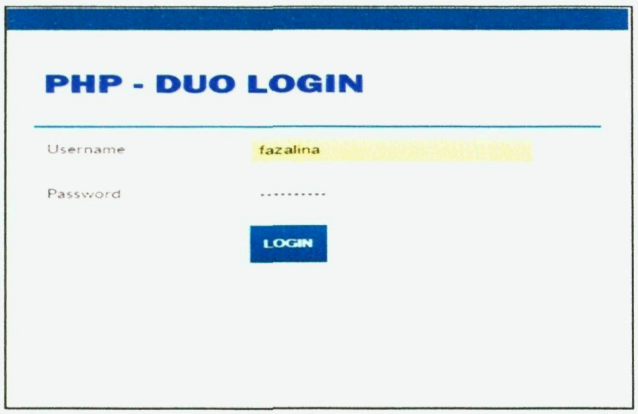

Fig. 6. Login screen when the user enters a username and password as they normally would.

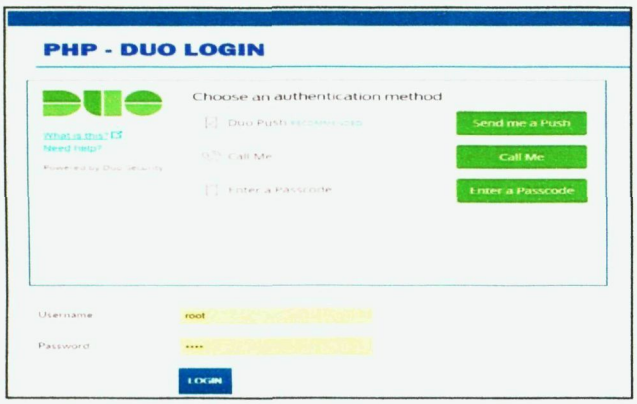

Fig. 7. Authentication method either using duo push notification, phone call or entering a passcode that sending via message.

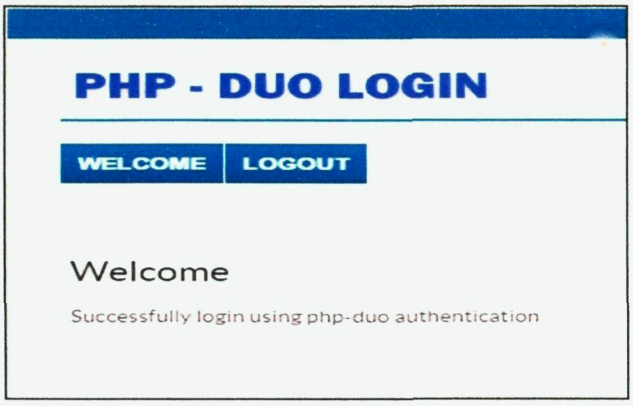

Fig. 8. Successfully login

B. Authentication Method

This section briefly explains the authentication method of duo mobile application as a second layer of security. In this project, it specifies into three authentication methods that users can choose which are duo push notification, call me and enter a passcode.

1) Duo push notification method – It can be seen in Figure 9. It is a push notification that is verifying and approving an authentication request from user. This method is a most easiest and faster than others method because of just clicking approve button. That is why this method recommended to choose.

2) Call me method - The server calling the user to give a passcode to verifying an authentication as shown in Figure 10.

3) Passcode method - It will be sending by a message to the user for authentication purpose as shown in Figure 11.

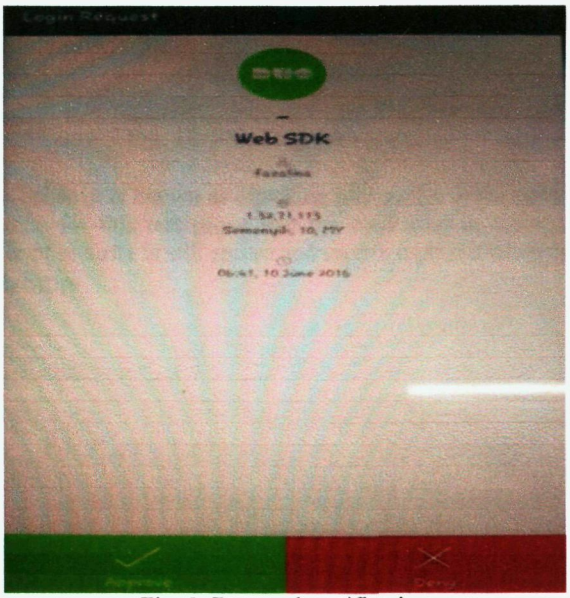

Fig. 9. Duo push notification

Fig. 10. Phone call notification

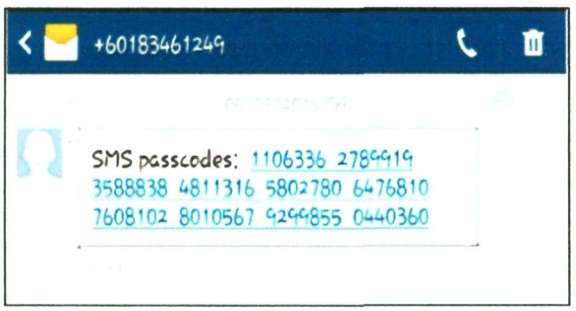

Fig. 11. Passcode sends via message

VI. DISCUSSION

This section presents the analysis on the proposed authentication system in mitigating few types of attack.

Table I shows the results based on the analysis conducted.

Type of attack	Descriptions	Successful Attack	
		First Layer of Security	Second Layer of Security (Duo Mobile Application)
A) DNS Spoofing - Ettercap	MTM - Sniffing of live connections	Successful (/)	Unsuccessful (X)
B) SSL Hijacking - SSL Strip with Ettercap	Hijacking http traffic – steal password	Successful (/)	Unsuccessful (X)
C) Session Hijacking - Hamster	Hijacking session – session cookies stolen	Successful (/)	Unsuccessful (X)

TABLE I: Types of attack and results

The results and analysis will be discussed in more details as per below:

A. DNS Spoofing

Fig. 11. Ettercap

Results for this test prove that the credential in the second layer of security is still secure and unable captured by using Ettercap. It only works in the first layer of security.

B. SSL Hijacking

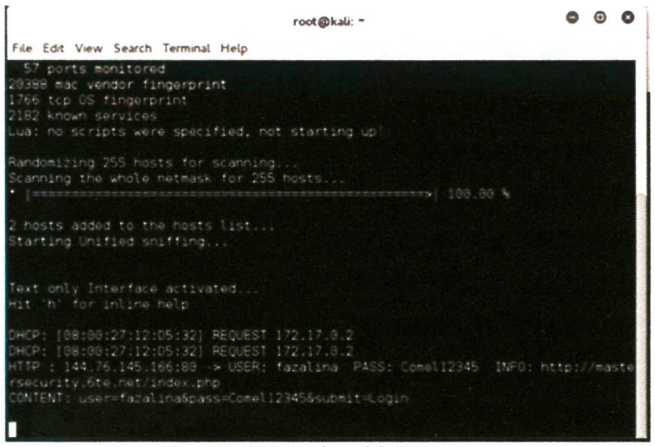

Fig. 12. SSL Strip with Ettercap

Ssl strip is known as hijacking http traffic in the network. Results for this test prove that the credential in the second layer of security is still secure and unable captured when using SSL Strip.

C. Session Hijacking

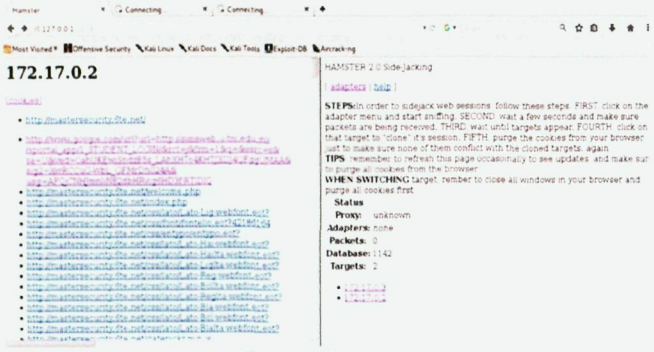

Fig. 13. Hamster

Cookies are small files which are stored on a user's computer. Results for this test illustrates that the second layer of security unsuccessful to hijack because of this application is setting their request timed out in shortly.

VII. CONCLUSION AND RECOMMENDATION

As a conclusion, duo mobile application software have been proven to enhance the security level at the authentication stage. Few attacks has been able to mitigate by using the proposed techniques. It is hope that, the proposed technique will increase the confident level of public users to utilize cloud services.

This study would help other researchers in the future for them to have the most effective way in focusing their research using other security methods to cover the first layer of security to get more secure on both levels, which is not just cover in the second layer of security part only and also can be improved in the interface of the login page just using the icon to give more practical, interactive and easy to use by users.

REFERENCES

[1] M. Ahmadi, M. Chizari, M. Eslami, M. Golkar and M. Vali, 'Access control and user authentication concerns in cloud computing environments', *2015 1st International Conference on Telematics and Future Generation Networks (TAFGEN)*, pp. 39 - 43, 2015.

[2] X. Tan and B. Ai, 'The issues of cloud computing security in high-speed railway', *Proceedings of 2011 International Conference on Electronic & Mechanical Engineering and Information Technology*, vol. 8, pp. 4358 - 4363, 2011.

[3] W. Liu, 'Research on cloud computing security problem and strategy', *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, pp. 1216–1219, 2012.

[4] Z. Javaid and I. Ijaz, 'Secure user authentication in cloud computing', *2013 5th International Conference on Information and Communication Technologies*, pp. 1–5, 2013.

[5] J. Yang and P. Lin, 'An ID-Based User Authentication Scheme for Cloud Computing', *2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 98–101, 2014.

[6] R. Banyal, P. Jain and V. Jain, 'Multi-factor Authentication Framework for Cloud Computing', *2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation*, pp. 105–110, 2013.

[7] K. Chachapara and S. Bhadlawala, 'Secure sharing with cryptography in cloud computing', *2013 Nirma University International Conference on Engineering (NUiCONE)*,pp. 1–3, 2013.

[8] F. FatemiMoghaddam, I. Ghavam, S. Varnosfaderani and S. Mobedi, 'A client-based user authentication and encryption algorithm for secure accessing to cloud servers based on modified Diffie-Hellman and RSA small-e', *2013 IEEE Student Conference on Research and Developement*, pp. 175–180, 2013.

[9] A. Dubey, A. Dubey, M. Namdev and S. Shrivastava, 'Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment', *2012 CSI Sixth International Conference on Software Engineering (CONSEG)*, pp. 1–8, 2012.

[10] C. Xue-Zhou, 'Network Data Encryption Strategy for Cloud Computing', *2015 Seventh International Conference on Measuring Technology and Mechatronics Automation*, pp. 693–697, 2015.

[11] Shaikh, F.B. and Haider, S., 'Security Threats in Cloud Computing', *6th International Conference on Internet Technology and Secured Transactions, 11-14 December 2011, Abu Dhabi, United Arab Emirates*,pp. 214–219, 2011.

[12] N. Yildirim and A. Varol, "Android based mobile application development for web login authentication using fingerprint recognition feature", *2015 23nd Signal Processing and Communications Applications Conference (SIU)*, pp. 2662 - 2665, 2015.

[13] T. Bhattasali and K. Saeed, "Two factor remote authentication in healthcare", *2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 380 - 386, 2014.

[14] M. Xie, Y. Li, K. Yoshigoe, R. Seker and J. Bian, "CamAuth: Securing Web Authentication with Camera", *2015 IEEE 16th International Symposium on High Assurance Systems Engineering*, pp. 232 - 239, 2015.

[15] Z. Abduljabbar, H. Jin, A. Yassin, Z. Hussien, M. Hussain, S. Abbdal and D. Zou, "Robust scheme to protect authentication code of message/image documents in cloud computing", *2016 International Conference on Computing, Networking and Communications (ICNC)*, pp. 1 - 5, 2016.

[16]G. Xie and B. Yao, "Cloud storage identity design based on fingerprint identification", 2013 6th International Conference on Information Management, Innovation Management and Industrial Engineering, vol. 1, pp. 569 - 572, 2013.

[17]U. Dubey, A. Trisal, J. Bose, M. Brabhui and N. Ahamed, "A hybrid authentication system for websites on mobile browsers", 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 266 - 270, 2014.

[18] J. Liu, M. Au, X. Huang, R. Lu and J. Li, "Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services",

IEEE Trans.Inform.Forensic Secur., vol. 11, no. 3, pp. 484-497, 2016.

[19]K. Martin and Wenyong Wang, "Aya: "An efficient access-controlled storage and processing for cloud-based sensed data"", 2015 12th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), pp. 130 - 134, 2015.

[20]S. El-Booz, G. Attiya and N. El-Fishawy, "A secure cloud storage system combining Time-based One Time Password and Automatic Blocker Protocol", 2015 11th International Computer Engineering Conference (ICENCO), pp. 188 - 194, 2015.